UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/671,671	09/28/2000	Young Hun Choi	P56173	7267

8439 7590 08/03/2006

ROBERT E. BUSHNELL
1522 K STREET NW
SUITE 300
WASHINGTON, DC 20005-1202

EXAMINER	
KRONENTHAL, CRAIG W	

ART UNIT	PAPER NUMBER
2624	

DATE MAILED: 08/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/671,671	CHOI ET AL.	
	Examiner	Art Unit	
	Craig W. Kronenthal	2624	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,12,13 and 15-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-9,12,13 and 15-23* is/are allowed.

6)☒ Claim(s) *24-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 7/18/06
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed June 5, 2006, has been entered and made of record.

2. The examiner withdraws the objections to claims 27, 29, and 31 in view of the amendment.

Response to Arguments

3. Applicant's arguments with respect to claims 24, 25, and 26 have been fully considered but they are not persuasive. Applicant argues in essence that O'Connor fails to suggest modifying Fitzpatrick to disclose that the kernel determines whether the fingerprint data base has been established in the information device, recognizes that the external device and the information device have been activated and performs a fingerprint registration routine when it is determined that the fingerprint data has not been established. The examiner disagrees and indicates that O'Connor's teaching of encoding the security feature into the BIOS is an example only, and not meant to limit the use of the security feature. Figure 5 just represents one embodiment of O'Connor's invention (col. 2 lines 44-46). O'Connor also discloses that the use of the security feature could be implemented by simply switching out a user's current mouse with a mouse capable of capturing fingerprints without having to make modifications to the BIOS (col. 3 lines 31-38). Furthermore, O'Connor discloses another embodiment in Figure 9, where the security features are implemented in an application (col. 6 lines 15-

37). The examiner also disagrees with the applicant's assertion that O'Connor teaches away from modifying Fitzpatrick's kernel. The examiner notes the applicant's recognition of O'Connor's motivation for implementing the security feature in the BIOS, specifically so that the security function cannot be defeated by loading from a floppy disk when the computer is "booted" (col. 3 lines 38-41). However, the examiner points out that O'Connor has also mentioned advantages and motivation for implementing the security features in an operating system, specifically so that the security processing may be run automatically at regular intervals even interrupting otherwise normal PC operation and operating programs to perform additional and continuing verification of user authorization (col. 7 lines 35-39).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 24, 25, and 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fitzpatrick et al. (PN 5,420,936, hereinafter Fitzpatrick) in view of O'Connor et al. (PN 5,838,306, hereinafter O'Connor) and Lane (PN 5,623,552, hereinafter Lane).

Regarding Claim 24: Fitzpatrick discloses an information device recognizing a fingerprint, the information device comprising:

- a fingerprint data base (access table) storing registered fingerprint data [The access table is found in the access grantor (Figure 4, 76; col. 4 lines 20-21).];
- a fingerprint verifying unit (fingerprint analyzer, Figure 4, 82) comparing fingerprint data (fingerprint image) transmitted (communicated) from an external device (monitor, 50) to the fingerprint verifying unit (82) [The fingerprint image is captured by the touch-sensitive surface (70) located on the monitor (50) and transmitted via the touch driver (74) to the fingerprint analyzer (82), which compares the image to the contents of the access table (col. 4 lines 16-21).]; and
- a kernel [A kernel is an inherent feature of an operating system.] of an operating system (Figure 4, 84) of the information device permitting access to a program stored in the information device when the fingerprint verifying unit determines that transmitted fingerprint data match the registered fingerprint data [The operating system (84) grants access to the appropriate program stored in the nonvolatile storage (88) when the access grantor (76) determines that a specified confidence level is met indicating a match (col. 4 lines 18-26).].

Fitzpatrick does not disclose the kernel checking the establishment of a data base, recognizing the external device, or determining if the external device is a fingerprint reader. However, O'Connor discloses a method for:

- determining whether the fingerprint data base (designated memory) has been established (contains any pre-approved signatures) in the information device (computer system shown in Figure 4) [This determining step is performed by the check fingerprint BIOS routine (501).].

It would have been obvious to one of ordinary skill in the art to modify Fitzpatrick's kernel to include the routine of O'Connor. Furthermore, one would have been motivated to make this modification to ensure that a touch screen monitor capable of reading fingerprints is connected as opposed to the typical monitor not having fingerprint reading capabilities.

O'Connor however, does not disclose performing the fingerprint registration routine when it is determined that the data base has not been established. Another reference to Lane discloses recognizing activation (Figure 14, 200, yes, col. 8 lines 35-37) and performing a fingerprint routine (fingerprint sensing, Figure 14, 201) when it is determined that the fingerprint data base (memory) has not been established (Figure 14, 210, no). Lane teaches performing fingerprint sensing "in any event" which includes when no fingerprint data is stored in memory (col. 8 lines 50-55). It would have been obvious to one of ordinary skill in the art to modify O'Connor's routine at step 505, which generates a 100% Valid return, to instead execute fingerprint sensing, as taught by Lane. Furthermore, one of ordinary skill in the art would have been motivated to make this modification to establish a memory with fingerprint data for future comparisons. This would especially be useful in the initial setup of the system to establish the administrator.

Regarding Claim 25: Fitzpatrick discloses an information device recognizing a fingerprint, the information device comprising:

- a fingerprint data base (access table) storing registered fingerprint data (see analogous arguments of claim 24);
- a kernel of an operating system (Figure 4, 84) of the information device (see analogous arguments of claim 24); and
- a fingerprint verifying unit (82) comparing fingerprint data transmitted (communicated) from an external device (monitor, 50) to the fingerprint verifying unit (82) and controlling the kernel [A kernel is an inherent feature of an operating system (84).] to execute a program stored in the information device when the fingerprint verifying unit (82) determines that the transmitted fingerprint data match the registered fingerprint data [The fingerprint analyzer (82) compares an input fingerprint image to the contents of an access table (col. 4 lines 16-21). The granting of access to an appropriate program, which is performed by the operating system (84), is dependent on the results of the comparison, and therefore, the fingerprint analyzer (82) controls the kernel (col. 4 lines 18-26).].

Fitzpatrick does not disclose the kernel checking the establishment of a data base, recognizing the external device, or determining if the external device is a fingerprint reader. However, O'Connor discloses a method for:

- determining whether the fingerprint data base (designated memory) has been established (contains any pre-approved signatures) in the information device

(computer system shown in Figure 4) [This determining step is performed by the check fingerprint BIOS routine (501).].

It would have been obvious to one of ordinary skill in the art to modify Fitzpatrick's kernel to include the routine of O'Connor. Furthermore, one would have been motivated to make this modification to ensure that a touch screen monitor capable of reading fingerprints is connected as opposed to the typical monitor not having fingerprint reading capabilities.

O'Connor however, does not disclose performing the fingerprint registration routine when it is determined that the data base has not been established. Another reference to Lane discloses recognizing activation (Figure 14, 200, yes, col. 8 lines 35-37) and performing a fingerprint routine (fingerprint sensing, Figure 14, 201) when it is determined that the fingerprint data base (memory) has not been established (Figure 14, 210, no). Lane teaches performing fingerprint sensing "in any event" which includes when no fingerprint data is stored in memory (col. 8 lines 50-55). It would have been obvious to one of ordinary skill in the art to modify O'Connor's routine at step 505, which generates a 100% Valid return, to instead execute fingerprint sensing, as taught by Lane. Furthermore, one of ordinary skill in the art would have been motivated to make this modification to establish a memory with fingerprint data for future comparisons. This would especially be useful in the initial setup of the system to establish the administrator.

Regarding Claim 27: Fitzpatrick discloses the information device according to claim 24, including an operating system inherently having a kernel. Fitzpatrick does not disclose the kernel checking the establishment of a data base, recognizing the external device, or determining if the external device is a fingerprint reader. However, O'Connor discloses a method for:

- determining whether the external device (mouse) is a fingerprint recognizing device when it is determined that the fingerprint data base (designated memory) has been established (there are signatures in the memory) [The routine has a decision block 509 for determining if the mouse is compatible with the security system, which is essentially determining if the mouse is capable of capturing fingerprints (col. 5 lines 25-30). Step 509 of the routine is only executed when it is determined at decision block 503 that there are signatures in memory (col. 5 lines 23-25).].

It would have been obvious to one of ordinary skill in the art to modify Fitzpatrick's kernel to include the routine of O'Connor. Furthermore, one would have been motivated to make this modification to ensure that a touch screen monitor capable of reading fingerprints is connected as opposed to the typical monitor not having fingerprint reading capabilities.

Regarding Claim 28: Fitzpatrick discloses the information device according to claim 27, wherein the external device comprises a monitor (50) including a fingerprint recognizing module including a fingerprint image recognizing unit (touch-sensitive surface, 70) and

transmitting the fingerprint data recognized by the fingerprint image recognizing unit to the information device (Figure 4, the combination of 76, 82, 84, and 88) [The touch-sensitive surface (70) recognizes a fingerprint, which is then transmitted via the touch driver (74) for processing by the information device comprising a fingerprint data base (access table found in the access grantor (76)), fingerprint verifying unit (82), kernel (found in the operating system (84)), and storage (88) (col. 4 lines 3-26).].

Regarding Claim 29: See the analogous arguments of claim 27.

Regarding Claim 30: See the analogous arguments of claim 28.

6. Claims 26, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fitzpatrick in view of Postlewaite et al. (PN 5,854,891, hereinafter Postlewaite), O'Connor, and Lane.

Regarding Claim 26: Fitzpatrick discloses an information device recognizing a fingerprint, the information device comprising:

- a fingerprint data base storing registered fingerprint data (see analogous arguments of claim 24);

- a fingerprint verifying unit comparing fingerprint data transmitted from an external device to the fingerprint verifying unit (see analogous arguments of claim 24); and
- a kernel of an operating system of the information device permitting access to a program through the information device when the fingerprint verifying device determines that the transmitted fingerprint data match the registered fingerprint data (see analogous arguments of claim 24).

Fitzpatrick does not disclose the program, which access may be permitted, to be related to electronic commerce. However, Postlewaite discloses the desire to prevent unauthorized access to computer programs controlling bank and other financial accounts (col. 1 lines 44-48), which are types of electronic commerce. It would have been obvious to one of ordinary skill in the art to modify Fitzpatrick to store programs in the nonvolatile storage (88) that are related to electronic commerce.

Fitzpatrick also does not disclose the kernel checking the establishment of a data base, recognizing the external device, or determining if the external device is a fingerprint reader. However, O'Connor discloses a method for:

- determining whether the fingerprint data base (designated memory) has been established (contains any pre-approved signatures) in the information device (computer system shown in Figure 4) [This determining step is performed by the check fingerprint BIOS routine (501).].

It would have been obvious to one of ordinary skill in the art to modify Fitzpatrick's kernel to include the routine of O'Connor. Furthermore, one would have been motivated

to make this modification to ensure that a touch screen monitor capable of reading fingerprints is connected as opposed to the typical monitor not having fingerprint reading capabilities.

O'Connor however, does not disclose performing the fingerprint registration routine when it is determined that the data base has not been established. Another reference to Lane discloses recognizing activation (Figure 14, 200, yes, col. 8 lines 35-37) and performing a fingerprint routine (fingerprint sensing, Figure 14, 201) when it is determined that the fingerprint data base (memory) has not been established (Figure 14, 210, no). Lane teaches performing fingerprint sensing "in any event" which includes when no fingerprint data is stored in memory (col. 8 lines 50-55). It would have been obvious to one of ordinary skill in the art to modify O'Connor's routine at step 505, which generates a 100% Valid return, to instead execute fingerprint sensing, as taught by Lane. Furthermore, one of ordinary skill in the art would have been motivated to make this modification to establish a memory with fingerprint data for future comparisons. This would especially be useful in the initial setup of the system to establish the administrator.

Regarding Claim 31: See the analogous arguments of claim 27.

Regarding Claim 32: See the analogous arguments of claim 28.

Allowable Subject Matter

7. Claims 1-9, 12, 13, 15-23 stand allowed.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Craig W. Kronenthal whose telephone number is (571) 272-7422. The examiner can normally be reached on 8:00 am - 5:00 pm / Mon. - Fri..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bhavesh Mehta can be reached on (571) 272-7453. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Craig W. Kronenthal
July 24, 2006

BHAVESH M. MEHTA
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600